Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for **2018** covering the prior calendar year **2017**.

1. Date filed: **February 22, 2018**

2. Name of company covered by this certification: **Working Assets Funding Service, Inc. dba Credo Long Distance on behalf of itself and its affiliate Credo Mobile, Inc.**

3. Form 499 Filer ID: **803457**

4. Name of signatory: **Trish Tobin**

5. Title of Signatory: **Chief Marketing Officer**

6. Certification:

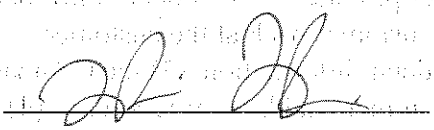
I, Trish Tobin, certify that I am an officer of the company named above and, acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. §64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions *(i.e.,* proceedings instituted or petitions filed by a company at either state commissions, in the court system, or at the Commission) against data brokers in the past year.

The company has received four customer complaints in the last year concerning the company's inadvertent release of a customer's CPNI to an unauthorized individual.

The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: 

Trish Tobin
Chief Marketing Officer

Attachments: Accompanying Statement explaining CPNI Procedures

DESCRIPTION OF CPNI OPERATING PROCEDURES AND POLICIES

- The Company's outbound telemarketing is performed by Company employees who use CPNI solely for the purpose of providing or marketing service offerings within the category of service to which the customer already subscribes, as permitted under the Commission's rules.

- Electronic files and databases containing CPNI are maintained on computers that are not accessible from the Internet without secure identification or that are on the Company's intranet behind firewalls that are regularly monitored and tested for effectiveness.

- Company employees are trained that customer information is confidential and private. Only those employees needing access to such information to perform their duties are able to use the database containing this information. Each employee having access is trained not to divulge customer information to any third party except the customer (pursuant to the safeguards described below) and certain outside vendors (*e.g.*, outside vendors perform billing services for the Company). All such vendors sign non-disclosure agreements restricting the use of customer information to only the purpose of their engagement by the Company.

- The Company has further instructed employees about the additional requirements established in the Commission's EPIC CPNI Order. If an employee discloses prohibited information to a customer, the Company will investigate the incident and determine whether the disclosure was intentional or accidental. If the disclosure was accidental, the Company will take immediate steps to reinforce the requirements with the employee and monitor that employee. If the Company determines that the disclosure was intentional, the employee will be terminated.

- It is the Company's policy that customer call detail not be disclosed to a customer on an inbound call unless: (1) the customer provides the call detail information in the first place, (2) the Company calls the customer back at the customer's telephone number of record with the call detail information, (3) the Company sends the call detail information to the customer's address of record, or (4) the customer provides a password that was initially established pursuant to the EPIC CPNI Order requirements.

- The Company notifies customers if it receives account information changes by sending a notice of change letter to customer's (unchanged) address of record for address changes or an email to customer's (unchanged) email address of record for online account information changes, asking the customer to call immediately if he or she did not authorize the change. The notice does *not* include changed information or reference account information.

- The Company has instructed its customer care vendor's service representatives about the requirements of the Commission's EPIC CPNI Order and engages in regular call monitoring to ensure compliance with these requirements. If a vendor service representative does not follow the requirements, the representative will be reprimanded and retrained on the requirements. If a representative does not follow the requirements a second time, that representative will be removed from the Company account.

- The Company provides online account access to customers. Online account access is password protected. The customer establishes a password. If a customer's online password is forgotten or lost, the Company uses a back-up customer authentication method that is *not* based on readily available biographical information or account information. Account access is blocked after repeated unsuccessful attempts to log into an account online.

- The Company refers all requests for CPNI from law enforcement, government agencies, etc. to its Legal Department. All requests require proper legal documentation (*e.g.*, a subpoena) before customer information is released.

- All Company employees are required to report any breach or potential breach of CPNI safeguards. In the event of a breach which results in CPNI being released to a third party, the Company will follow the Commission's rules regarding notification to law enforcement and to the customer whose CPNI was released. The Company will keep records of any disclosed breaches, law enforcement notifications and law enforcement responses for at least two (2) years.